

ONE HUNDRED FIFTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

December 18, 2017

Mr. Jeremy A. Grant
Managing Director
Technology Business Strategy
Venable, LLP
600 Massachusetts Avenue, N.W.
Washington, DC 20001

Dear Mr. Grant:

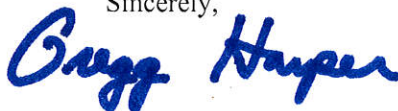
Thank you for appearing before the Subcommittee on Oversight and Investigations on November 30, 2017, to testify at the hearing entitled "Identity Verification in a Post-Breach World."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Monday, January 8, 2018. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Ali.Fulling@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Gregg Harper
Chairman
Subcommittee on Oversight and Investigations

cc: The Honorable Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

Attachment—Additional Questions for the Record

The Honorable Morgan Griffith

1. In your testimony, you discussed how certain government agencies like the Social Security Administration are well-poised to help address the online identity challenges we're discussing today. You discuss a hypothetical service that the SSA could offer that would be valuable to both consumers and businesses looking for identity authentication mechanisms that would essentially make SSA's current process digital.
 - a. Drawing on your government experience, how would SSA – or a government agency with similar potential – go about creating these types of systems and services?
 - b. What do you think the cost might be of implementing such systems, both in time and resources?
2. The federal government is not exactly well-known for successfully designing and implementing complex, large-scale systems such as the one you're describing.
 - a. Do you believe that the federal government has the resources and capabilities it needs to implement such systems?
 - b. Beyond resources and expertise, does the federal government have a plan for designing and implementing such systems, or would agencies tasked with these kinds of projects be starting from scratch?
 - c. What are some of the potential pitfalls of the government undertaking such a project?
3. As we understand it, the FIDO Alliance has already published several standards.
 - a. Can you give us some examples of FIDO standards, and what these standards allow organizations to do?
 - b. We've heard that organizations are now releasing "FIDO-compatible" products, in some cases. Can you give us some examples?
 - i. Do you have a sense of how expensive these types of standards and techniques are to deploy in company products, both in time and resources?
4. An issue that we tend to see with efforts to address cybersecurity issues broadly, not just identity issues, is that proposed solutions are often proprietary, which limits the ability of smaller companies and developers to leverage them.
 - a. Are FIDO Alliance standards proprietary?
 - b. How does an organization – large, small, or maybe just a single individual – access FIDO Alliance standards?

5. I understand that you led the development of the National Strategy for Trusted Identities in Cyberspace, or NSTIC, on behalf of NIST. The NSTIC was published in 2011, six years ago. Obviously, the situation has developed since then, not simply with regards to the types of information and connected devices that are available on the Internet, but in the sheer number of compromised PII records available.
 - a. How does this affect the findings from the NSTIC, if at all?
 - b. Are you aware of any work to update the NSTIC? Is it a living document that gets updated regularly?
6. I realize that you're no longer with NIST, but we understand that you are generally still well informed about their current efforts.
 - a. Could you tell us a little more about the Trusted Identities Group, how it relates to the NSTIC, and how the TIG is working to bring advanced identity verification mechanisms to the federal government and private sector?
7. In your testimony, you mentioned that funding for NIST's efforts in this space is being cut.
 - a. Do you have a sense of why?
 - b. Is it funding for pilots that will be affected, or the office itself?
 - i. What are some of the dangers of the lack of funding?